

ABSTRACT

[0105] The spam blocker monitors the SMTP/TCP/IP conversation between a sending message transfer agent MTA_0 and a receiving message transfer agent MTA_1; catches MTA_0's IP address IP_0, MTA_0's declared domain D_0, from-address A_0; and to-address A_1; and uses this source and content based information to test for unsolicited messages. It interrupts the conversation when MTA_0 sends a RCPT command and uses the various test results to decide if the message is suspected of being unsolicited.

[0106] If the message is suspected of being unsolicited and to-address is not in the save_spam database then the spam blocker logs the rejected message, sends an error reply to MTA_0 which forces MTA_0 to terminate the connection before the body of the message is transmitted. If the message is suspected of being unsolicited and to-address is in the save_spam database then the spam blocker logs the rejected message, substitutes a diversion address A'_1 for the to-address A_1 in the RCPT command, and send the modified RCPT command to MTA_1 and allows the conversation to continue. If the message is not suspected of being unsolicited then the spam blocker logs the allowed message, releases the intercepted RCPT command which allows the conversation to continue.